UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,444	07/05/2001	Elsie Van Herreweghen	CH920000009US1	4090

7590 07/06/2009

Steven Fischman, Esq
SULLY SCOTT MURPHY & PRESSER
400 Garden City Plaza
Suite 300
Garden City, NY 11530-3319

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
07/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ELSIE VAN HERREWEGHEN

Appeal 2008-005154
Application 09/899,444
Technology Center 2400

Decided:[1] July 6, 2009

Before JOHN A. JEFFERY, ST. JOHN COURTENAY III,
and STEPHEN C. SIU, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-15, 17-28, and 30-35. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellant invented a system for securely proving ownership of anonymous or pseudonymous receipts such that a party that proves its ownership of the receipt can stay anonymous. Specifically, a sender sends a first message to a first addressee including a transaction request and references an owner of a receipt to be generated. The first addressee returns a signed receipt including the reference and the details for what receipt has been given. The sender sends a second message including the receipt to a second addressee who then (1) obtains a public signature verification key on the basis of the reference to receipt's owner, and (2) authenticates the second message.[2] Claim 6 is illustrative:

6. A receipt generation method, comprising generating an electronic receipt in a communication system providing a public key encryption system, including the steps of:

receiving a message from a sender using a pseudonym, wherein said pseudonym is issued using a first private-public signature key pair, and said message is electronically signed by said sender using the first private signature key owned by said sender, whereby said message includes a transaction request and a reference to a designated owner of a receipt to be generated;

authenticating said message using a public signature verification key associated to said first private signature key held by said sender of said message;

---

[2] *See generally* Abstract; Spec. 3.

issuing a receipt including said reference to said designated owner of said receipt and details for what said receipt has been given to provide said designated owner with said receipt and thereby to enable said owner to verify ownership of the receipt by using a second private-public signature key pair different than the first private-public signature key pair, while maintaining said owner anonymous or pseudonymous; and

electronically signing and issuing said receipt using the second private-public signature key pair assigned to an issuer issuing said receipt.

The Examiner relies on the following as evidence of unpatentability:

Brands[3]	US 5,604,805	Feb. 18, 1997
Muftic	US 5,850,442	Dec. 15, 1998
Lewis	US 6,233,565 B1	May 15, 2001
Ellison	US 6,976,162 B1	Dec. 13, 2005 (filed June 28, 2000)

1. The Examiner rejected claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34, and 35 under 35 U.S.C. § 103(a)[4] as unpatentable over Lewis, Ellison, and Brands. Ans. 3-10.
2. The Examiner rejected claims 1-5, 23, 24, 30, and 33 under 35 U.S.C. § 103(a) as unpatentable over Lewis, Muftic, and Ellison. Ans. 10-16.
3. The Examiner rejected claims 12, 14, 15, and 18 under 35 U.S.C.

---

[3] Although the Examiner and Appellant erroneously refer to this reference as "Brand," (*see, e.g.*, Br. 8; *see also* Ans. 3), we refer to its correct name "Brands."

[4] Although the Examiner indicates the statutory basis for this rejection was under § 102 in the statement of the rejection (Ans. 3), we presume the Examiner intended the statutory basis to be § 103 based on the record before us. Accordingly, we deem the Examiner's error harmless.

§ 103(a) as unpatentable over Lewis, Ellison, Brands, and Muftic. Ans. 13-16.[5]

Rather than repeat the arguments of Appellant or the Examiner, we refer to the Brief and the Answer[6] for their respective details. In this decision, we have considered only those arguments actually made by Appellant. Arguments which Appellant could have made but did not make in the Brief have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

THE OBVIOUSNESS REJECTION OVER LEWIS, ELLISON, AND BRANDS

Regarding representative claim 6,[7] the Examiner finds that Lewis discloses a receipt generation method with all of the claimed subject matter except for issuing a pseudonym using a first private-public key pair and the receipt enables the owner to verify ownership of the receipt while maintaining the owner anonymous or pseudonymous. The Examiner, however, relies on Ellison for this feature in concluding the claim would have been obvious. Ans. 3-4. The Examiner also relies on Brands for

[5] Although the Examiner's statement of the rejection includes claim 16 (Ans. 13), that claim has been cancelled. Br. 3. We nevertheless deem this error harmless.

[6] Throughout this opinion, we refer to the Appeal Brief filed August 10, 2007 and the Examiner's Answer mailed October 17, 2007.

[7] Appellant argues claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34, and 35 together as a group. *See* Br. 8-12. Accordingly, we select claim 6 as representative. *See* 37 C.F.R. § 41.37(c)(1)(vii).

teaching using a second private-public key pair to verify ownership of the receipt. Ans. 4-5.

Appellant argues that the Examiner's rejection is improper since the Examiner did not identify specific reasons in any of the references that would have prompted skilled artisans to combine the references. Br. 9. Appellant adds that even if the references could be combined, the combination does not teach or suggest every claimed limitation, namely (1) issuing and verifying a receipt while maintaining the owner anonymous or pseudonymous, and (2) using first and second private-public signature key pairs, where the user and receipt issuer exchange information using the first key pair, and the receipt issuer and owner communicate using the second key pair. Br. 9-11.

The issues before us, then, are as follows:

ISSUES

(1) Under § 103, has Appellant shown that the Examiner erred in rejecting claim 6 by finding that Lewis, Ellison, and Brands collectively teach or suggest a receipt generation method including (1) issuing and verifying a receipt while maintaining the owner anonymous or pseudonymous, and (2) using first and second private-public signature key pairs, where the user and receipt issuer exchange information using the first key pair, and the receipt issuer and owner communicate using the second key pair?

(2) Is the Examiner's reason to combine the teachings of these references supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence:

Lewis

1. Lewis discloses a system for conducting Internet-based financial transactions between a client and server. In response to the client and server being authenticated, the client issues a transaction request to the server. In response, the transaction server executes an electronic payment transaction at the server and records the transaction in a database. The server generates a receipt and transmits it to the client. Lewis, Abstract; col. 4, ll. 20-33.

2. The receipt includes the client digital signature and a data set uniquely identifying the executed transaction. Lewis, Abstract; col. 4, ll. 33-35.

3. In one embodiment, the transaction request can include the client digital signature, and the receipt can include the server digital signature. Lewis, col. 4, ll. 39-43.

4. Regarding authentication, the client may have a client public key and client private key. Likewise, the server may have a server public key and a server private key. Therefore, the public and private keys of both the client and the server are used to perform authentication. Lewis, col. 5, ll. 10-25.

Ellison

5. Ellison discloses a system that protects the identity of a platform by creating and using pseudonyms.[8] Specifically, a first platform 110 communicates with a second platform 120 via link 130. Upon user request, the first platform generates and transmits a pseudonym public key 14 to the second platform. The second platform then certifies that the pseudonym public key was generated by a trusted device 150 within the first platform. Ellison, col. 1, l. 66 – col. 2, l. 1; col. 3, ll. 1-13; Fig. 1.

6. Trusted device 150 includes an asymmetric key pair 220 including a public key (PUKP1) 230 and private key (PRKP1) 240. Device 150 may also include a public key 250 (PUKP2) of the second platform. Ellison, col. 3, ll. 36-41; Fig. 2.

7. Figures 4 and 5 of Ellison detail the process of producing and certifying pseudonyms. Upon receiving a user request, a pseudonym is produced, and a pseudonym public key (PPUKP1) is placed in a digital certificate template. Fig. 4, steps 400 and 405. After creating a certificate request with a "blinded" hash value, the certificate request is digitally signed with the private key (PRKP1) of the first platform. Fig. 4, steps 415-425. A device certificate (i.e., a digital certificate chain that includes the public key (PUKP1) of the first platform) is obtained to accompany the signed certificate request. Fig. 4, step 430. Both the signed certificate request and

[8] "A 'pseudonym' is an alias identity in the form of an alternate key pair used to establish protected communications with another platform and to identify that its platform includes trusted device 150." Ellison, col. 3, ll. 46-50.

device certificate are encrypted with the second platform's public key (PUKP2) and sent to the second platform. Fig. 4, steps 435 and 440. Ellison, col. 4, ll. 15-49; Figs. 4 and 5.

8. At the second platform, the signed certificate request and device certificate are recovered after decryption using the second platform's private key (PRKP2). Fig. 5, step 445. Then, the first platform's public key is obtained using a public key of a certification authority. Fig. 5, step 450. After recovering the certificate request and verifying the device certificate, the transformed certificate hash value is digitally signed to produce a "signed result" that is sent to the first platform. Fig. 5, steps 455-475. After performing an inverse transformation of the signed result, a digital signature of the certificate hash value is recovered and stored with one or more pseudonyms for subsequent communications with other platforms. Fig. 5, step 480. Ellison, col. 4, l. 50 – col. 5, l. 9; Fig. 5.

Brands

9. Brands teaches that a "blind" signature protocol can be used to guarantee privacy between a user and a certifying party. In one implementation, users are known by different pseudonyms at different organizations such that the pseudonyms are unlinkable. To this end, the user can transform an ordinary digital signature on one of his pseudonyms to a digital signature on each of his other pseudonyms. As such, information certified by one organization can be shown to all other organizations at which the user has a pseudonym without enabling the organizations to link the transferred information. Brands, col. 2, ll. 6-33.

Appellant's Disclosure

10. According to Appellant's Specification, once the sender receives the receipt from the first addressee, it is transferred from the sender to the designated owner of the receipt if the sender is different from the designated owner. But if the sender is the designated owner, the owner composes a second message including the receipt, signs it using a second secret signature key and sends it to a second addressee. Spec. 7:20-27.

PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966) (noting that 35 U.S.C. § 103 leads to three basic factual inquiries: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; and (3) the level of ordinary skill in the art). Furthermore, the Examiner's obviousness rejection must be based on

> "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" . . . . [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.

KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

If the Examiner's burden is met, the burden then shifts to the Appellant to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

"The motivation [to combine references] need not be found in the references sought to be combined, but may be found in any number of sources, including common knowledge, the prior art as a whole, or the nature of the problem itself." *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1361 (Fed. Cir. 2006) (citation omitted).

ANALYSIS

Based on the record before us, we find no error in the Examiner's obviousness rejection of representative claim 6. We begin by noting that nothing in the claim precludes the sender and the receipt owner from being the same entity. Indeed, the Specification contemplates this possibility (*see* FF 10) as does the Examiner. *See* Ans. 18 (labelling the user as the owner of the receipt).

Turning to the prior art, the Examiner relies on Lewis for the fundamental teaching of using two public-private key pairs in an Internet-based financial transaction involving a client and server in which a receipt is requested and generated. Ans. 17. The Examiner finds that a request for a receipt in Lewis is signed using a "client signature key" (a public-private key), and that the generated receipt is signed using an "issuer's signature key" (a public-private key). *Id.* That is, two public-private keys are used in

this transaction. We find no error in this position, particularly since Lewis teaches that the public and private keys of both the client and the server can be used to perform authentication. FF 4. Moreover, Lewis notes that the transaction request can include the client digital signature, and the receipt can include the client and server digital signatures. FF 2-3.

While these two key pairs in Lewis may not maintain the user anonymous or pseudonymous as Appellant argues (Br. 10), we find no error in the Examiner's position that such a feature would have been obvious in view of Ellison and Brands. Ellison uses pseudonyms to protect a platform's identity by generating a pseudonym public key that is transmitted to the second platform which, in turn, certifies that the pseudonym public key was generated by a trusted device in the first platform. FF 5. Notably, not only is a pseudonym public key used as part of this process, but also the first and second platform's public and private keys are utilized. *See* FF 5-8. As such, we see no reason why this technique involving pseudonyms could not be applied to Lewis' system to maintain privacy and protect the identity of platforms involved in such transactions.

We are also not persuaded of error in the Examiner's reliance on Brands for suggesting that different pseudonym key pairs could be utilized to ensure unlinkability of the respective transactions between (1) a user and the organization issuing the receipt, and (2) the user (i.e., the owner) and the organization verifying the receipt. Ans. 18. As Brands indicates, users can have different pseudonyms such that information certified by one organization can be shown to all other organizations at which the user has a pseudonym without enabling the organizations to link the transferred information. FF 9. This teaching further bolsters the Examiner's position

that using different private-public signature key pairs for exchanging information between (1) a user and receipt issuer, and (2) a receipt issuer and owner (which can be the user), respectively, would have been obvious to skilled artisans.

Moreover, we find that the Examiner's reason to combine the teachings of these references is supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion. Although Appellant argues that the references themselves do not contain such a motivation (Br. 9), we note that the reason to combine references need not be limited to the four corners of the cited references, but rather can be ascertained from any number of sources, including common knowledge, the prior art as a whole, or the nature of the problem itself. *See DyStar*, 464 F.3d at 1361. The Examiner's articulated basis for combining the references is rational in our view, and would reasonably have been derived from at least the common knowledge in the art.

For the foregoing reasons, Appellant has not persuaded us of error in the Examiner's rejection of representative claim 6. Therefore, we will sustain the Examiner's rejection of that claim, and claims 7-11, 13, 17, 19-22, 25-28, 31, 32, 34, and 35 which fall with claim 6.

THE OBVIOUSNESS REJECTION OVER LEWIS, MUFTIC, AND ELLISON

Regarding representative claim 1,[9] the Examiner finds that Lewis discloses all of the claimed subject matter except for (1) expressly teaching

[9] Appellant argues claims 1-5, 23, 24, 30, and 33 together as a group. *See* Br. 12-14. Accordingly, we select claim 1 as representative. *See* 37 C.F.R. § 41.37(c)(1)(vii).

how the receipt is authenticated, and (2) verifying receipt ownership while maintaining the user anonymous or pseudonymous. The Examiner, however, relies on Muftic for teaching verifying the authenticity of messages via a public key encryption scheme where the public key can be obtained via a digital certificate in concluding that the claim would have been obvious. Ans. 10-12 and 19. The Examiner also relies on Ellison for teaching using a pseudonym public key to sign the various transactions to maintain privacy. Ans. 12 and 20.

Appellant argues that there is no teaching, suggestion, or motivation to combine the references in the prior art. Br. 12-13. Appellant adds that even if the references could be combined, they do not teach or suggest the recited verification method involving issuing and verifying ownership of a receipt while maintaining the owner anonymous or pseudonymous using the first and second public-private key pairs as claimed. Br. 13-14.

The issues before us, then, are as follows:

ISSUES

(1) Under § 103, has Appellant shown that the Examiner erred in rejecting claim 1 by finding that Lewis, Muftic, and Ellison collectively teach or suggest a receipt ownership verification method including (1) issuing and verifying ownership of a receipt while maintaining the owner anonymous or pseudonymous, and (2) using first and second private-public signature key pairs, where the user and receipt issuer exchange information using the first key pair, and the receipt issuer and owner communicate using the second key pair?

(2) Is the Examiner's reason to combine the teachings of these references supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

FINDINGS OF FACT

The record supports the following additional findings of fact (FF) by a preponderance of the evidence:

Muftic

11. Muftic discloses an authentication process where the recipient's public key is obtained from a trusted third party. The trusted third party can sign the recipient's public key using the trusted third party's private key and therefore verify the integrity of the recipient's public key. Muftic, col. 3, ll. 30-52.

12. Muftic discusses various proposals addressing privacy enhancement for Internet electronic mail and certificate-based key management. These proposals include concepts used in the CCITT 1988 Recommendation X.509 directed to an authentication framework. Muftic, col. 4, ll. 27-32.

ANALYSIS

We will sustain the Examiner's obviousness rejection of representative claim 1. Our previous discussion regarding Lewis and Ellison applies equally here and we incorporate that discussion by reference. We reiterate, however, that while the two key pairs in Lewis may not maintain the user anonymous or pseudonymous as Appellant argues (Br. 13), we find

no error in the Examiner's position (Ans. 12, 19, and 20) that such a feature would have been obvious in view of Ellison's use of pseudonyms. As we indicated previously, Ellison's technique protects a platform's identity by generating a pseudonym public key that is transmitted to the second platform which, in turn, certifies that the pseudonym public key was generated by a trusted device in the first platform. FF 5.

We also see no error in the Examiner's reliance on Muftic (Ans. 10, 11, and 19) for teaching the use of digital certificates to obtain a public signature verification key in verifying ownership of a receipt as claimed. In this analysis, the Examiner relies extensively on Muftic's use of a public key encryption infrastructure and public keys distributed via digital certificates which can employ the X.509 protocol (Ans. 19)—a protocol that is at least suggested by Muftic. *See* FF 12. Notably, the Examiner's findings regarding the X.509 protocol used in connection with digital certificates are undisputed. In any event, we see no error in the Examiner's position, particularly since Muftic teaches that a recipient's public key can be obtained from a trusted third party that can sign the recipient's public key using the trusted third party's private key to verify the integrity of the recipient's public key. FF 11.

We also find that the Examiner's reason to combine the teachings of these references is supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion. Although Appellant argues that the references themselves do not contain such a motivation (Br. 12-13), we reiterate that the reason to combine references can be ascertained from any number of sources, including common knowledge, the prior art as a whole, or the nature of the problem itself. *See*

DyStar, 464 F.3d at 1361. The Examiner's articulated basis for combining the references to arrive at the invention of claim 1 is rational in our view, and would reasonably have been derived from at least the common knowledge in the art.

For the foregoing reasons, Appellant has not persuaded us of error in the Examiner's rejection of representative claim 1. Therefore, we will sustain the Examiner's rejection of that claim, and claims 2-5, 23, 24, 30, and 33 which fall with claim 1.[10]

THE OBVIOUSNESS REJECTION OVER LEWIS, ELLISON, BRANDS, AND MUFTIC

Likewise, we will sustain the Examiner's obviousness rejection of claims 12, 14, 15, and 18 over Lewis, Ellison, Brands, and Muftic. Although Appellant presents separate arguments for these claims, the arguments are essentially the same as those indicated for independent claims 6 and 13. *See* Br. 15-16. We are therefore not persuaded that the Examiner erred in rejecting claims 12, 14, 15, and 18 for the same reasons discussed above with respect to claims 6 and 13. The rejection is therefore sustained.

[10] Although Appellant presents an argument directed to Brands in connection with the Examiner's rejection of claim 1 (Br. 14), the Examiner did not rely on Brands in rejecting that claim. *See* Ans. 10. We therefore will not address this argument here.

CONCLUSION

Appellant has not shown that the Examiner erred in rejecting claims 1-15, 17-28, and 30-35 under § 103.

ORDER

The Examiner's decision rejecting claims 1-15, 17-28, and 30-35 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

Steven Fischman, Esq
SULLY SCOTT MURPHY & PRESSER
400 Garden City Plaza
Suite 300
Garden City NY 11530-3319